UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,404	06/13/2000	Nicolas J. Hammond	14102.0002	5767

23859 7590 01/02/2004

NEEDLE & ROSENBERG, P.C.
SUITE 1000
999 PEACHTREE STREET
ATLANTA, GA 30309-3915

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 01/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/592,404	HAMMOND, NICOLAS J.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☒ Claim(s) *10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1 through 10 are presented for examination.

Drawings

2. The drawings received on 13 June 2000 are accepted by the Examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 7 and 8 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,185,689 to Todd, Sr. et al., hereinafter Todd.

5. As per claim 7, Todd teaches a method of auditing security of a computer system, comprising the steps of:

a. receiving from a user, via a global computer network, an instruction to perform a security audit scan on a computer system (Figures 1, 2 [blocks 34, 36, 38], 3 [block 32, 36], 6, 7, 8; column 4, lines 7-13; column 6, lines 21-26; column 6, lines 50-56);

b. instructing a scanning machine to access the remote computer system via the global computer network and thereby perform a security audit scan of the remote computer system (Figures 6, 7, 8; column 4, lines 14-19; column 7, lines 32-56); and

c. reporting at least one result of the security audit scan to the user once the security audit scan is complete (Figures 6, 7, 8; column 7, lines 53-56; column 7, lines 61-65; column 8, lines 2-6).

6. Regarding claim 8, Todd teaches further comprising the step of recording the result of the security audit in a computer memory (column 7, lines 57-65). Todd discloses a file that contains results of the security audit being created on the server.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1 through 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,205,552 to Fudge, hereinafter Fudge, in view of Todd.

9. As per claim 1, Fudge teaches an apparatus for auditing security of a remote computer system, comprising:

b. a plurality of scanning machines in communication with the global computer network and programmed to execute selectively a security audit scan of the remote computer system via the global computer network (Figure 1 [block 160]; column 3, lines 47-59); and

c. a central computer, having a memory, configured as a database server and as a scheduler, in communication with the secure application server and the scanning machine

(Figures 1 [block 120], 2 [blocks 212, 214, 218]; column 3, lines 19-33; column 4, lines 21-41; column 4, lines 61-67), programmed to perform the following operations:

a. evaluate a database to determine if a security audit scan is currently scheduled to be run for a user (Figure 1 [block 152]; column 3, lines 56-59; column 4, line 35-42; column 4, lines 61-67);

b. determine which of the plurality of scanning machines is available to perform a security audit scan (Figure 1 [block 160]; column 3, lines 47-59);

c. copy scan-related information into a scanning machine determined to be available and instruct the scanning machine to begin scan (Figures 2 [block 218], 3 [blocks 304, 306]; column 4, lines 47-54); and

d. record the results of the scan in the memory (Figure 3 [block 306]; column 4, lines 47-54).

Fudge does not teach a plurality of scanning machines. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the single scanning machine of Fudge to multiply the effects of the scanning machine. One would be motivated to have multiple scanning machines in order to process a plurality of security audits, thereby creating a more efficient and cost effective system able to service multiple clients simultaneously. It would still be further obvious to choose one of the plurality of scanning machines based on location or services provided, such as a variety of attacks offered on said machine. See MPEP § 2144.04; see also *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960). Fudge does explicitly disclose evaluating a database to determine if a security audit is scheduled to be run. Yet Fudge suggests a method of performing a security audit

periodically, whether it be an hourly, daily, weekly, or monthly basis. Fudge does not disclose a notification mechanism to trigger the vulnerability scan. Therefore, one of ordinary skill would use a database to trigger the vulnerability scanner based on the last time the vulnerability assessment was performed on network resource.

10. Fudge does not teach:

a. at least one secure application server in communication with a global computer network and programmed to receive selectively security audit instruction data from the remote computer system via the global computer network.

11. Todd teaches:

a. at least one secure application server in communication with a global computer network and programmed to receive selectively security audit instruction data from the remote computer system via the global computer network (Figures 1 [block 26], 2 [blocks 34, 38], 3 [block 32]; column 4, lines 7-19; column 6, lines 14-26). Fudge discloses a workstation attached to the scanning machine and central computer as an interface for users who would want to initiate, monitor, control or review the analysis performed on the network being audited. It would have been obvious to one of ordinary skill in the art at the time the invention was made to replace the workstation of Fudge with the Internet server disclosed in Todd. Replacing the workstation with the Internet server allows a multitude of users to assess the security of their networks, either home or corporate, or machines and devices connected to the Internet, thereby creating a larger client base.

12. Regarding claim 2, Todd teaches wherein the secure application server comprises a Web server (column 6, lines 14-17).

13. Regarding claim 3, Todd teaches wherein the central computer is further programmed to notify the user via e-mail that a scan is commencing (Figures 3 [block 42], 7 [block 42]; column 6, lines 40-49).

14. Regarding claim 4, Fudge teaches wherein the central computer is further programmed to update database to indicate that scan is complete (Figure 1 [blocks 150, 152]; column 3, lines 56-59; column 4, lines 61-67).

15. Regarding claim 5, Todd teaches wherein the central computer is further programmed to notify the user of a completion of a scan (column 7, lines 47-56).

16. Regarding claim 6, Fudge teaches wherein when the central computer performs the operation in which the central computer records the results of the scan, the central computer also copies the data to the database and copies the report to the file system on the database machine when scan is complete (Figure 1 [blocks 150, 152]; column 3, lines 56-59; column 4, lines 61-67).

17. Claim 9 is rejected under 35 U.S.C. 103(a) as being obvious over Todd.

18. Regarding claim 9, Todd does not teach teaches further comprising the step of evaluating which of a plurality of scanning machines is available to perform the security audit scan. Todd does not teach a plurality of scanning machines, yet only teaches one scanning machine. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the single scanning machine of Todd. One would be motivated to have multiple scanning machines in order to process a plurality of security audits, thereby creating a more efficient and cost effective system able to service multiple clients simultaneously. It would still be further obvious to choose one of the plurality of scanning machines based on location or services provided, such as a variety of attacks offered on said machine. See MPEP § 2144.04; see also *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

19. Claim 10 is rejected under 35 U.S.C. 103(a) as being obvious over Fudge.

20. As per claim 10, Fudge teaches a method of auditing computer system security, comprising the steps of:

a. accessing a database to determine when a security audit scan of a computer system is to be executed (Figure 1 [block 152]; column 3, lines 56-59; column 4, line 35-42; column 4, lines 61-67);

b. upon determining that a security audit scan of the remote computer system is to be executed (Figure 1 [block 152]; column 3, lines 56-59; column 4, line 35-42; column 4, lines 61-67), performing the following steps:

i. copying security audit scan data into a scanning system (Figures 2 [block 218], 3 [blocks 304, 306]; column 4, lines 47-54);

ii. causing the scanning system to establish communication with the remote computer system via a global computer network (Figure 2 [blocks 202, 204, 206]; column 3, line 63 to column 4, line 7; column 4, lines 43-47);

iii. causing the scanning system to execute a security audit scan of the remote computer system via the global computer network (Figure 3 [block 302]; column 4, lines 43-54); and

iv. storing a result of the security audit scan of the global computer network (Figures 1 [blocks 150, 152], 3 [block 306]; column 3, lines 54-59; column 4, lines 48-54); and

c. transmitting a message to a user of the remote computer system that indicates the result of the security audit scan (Figure 3 [block 312]; column 4, lines 56-67). Fudge does explicitly disclose evaluating a database to determine if a security audit is scheduled to be run. Yet Fudge suggests a method of performing a security audit periodically, whether it be an hourly, daily, weekly, or monthly basis. Fudge does not disclose a notification mechanism to trigger the vulnerability scan. Therefore, one of ordinary skill would use a database to trigger the vulnerability scanner based on the last time the vulnerability assessment was performed on network resource.

Claim Objections

21. Claim 10 is objected to because of the following informalities: there is two step b's. Appropriate correction is required. For the purposes of examination the second step b will be considered step c.

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

23. The following patents are cited to further show the state of the art with respect to network security auditing systems, such as:

United States Patent No. 5,961,644 to Kurtzberg et al., which is cited to show a method for testing the integrity of computer security alarm systems.

United States Patent No. 6,282,546 to Gleichauf et al., which is cited to show a method for real-time insertion of data into a database for network intrusion detection and vulnerability assessment.

United States Patent No. 6,324,656 to Gleichauf et al., which is cited to show a method for a rules-driven multi-phase network vulnerability assessment.

United States Patent No. 6,535,227 to Fox et al., which is cited to show a method for assessing the security of a network with a graphical user interface.

United States Patent No. 6,574,737 to Kingsford et al., which is cited to show a system for penetrating computer networks.

United States Patent No. 6,321,338 to Porras et al., which is cited to show a network surveillance system.

United States Patent No. 6,484,203 to Porras et al., which is cited to show an event monitoring system.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

26. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100